



Datenschutz-Zertifikat – nur sicher mit dem Siegel?

mit ISO 27701 . Dr.tech Wolfgang Prentner . IT-Ziviltechniker . Informatiker .
Gerichtssachverständiger

Do. 25.2.2021. Webinar . Online Präsentation

CYBERBELT[®]

IHR INTERNET-SICHERHEITSGURT

cyberbelt.net



Sicherheits-Audit

Pentesting

Social Hacking

Red Team Operations

Code Analysen

mit **Zertifikat**

ZITP 



Wir übernehmen die Kontrolle
Ihrer Unternehmensnetzwerke und Daten!

SOCIAL HACKING
Red Team Operations

ZfP 
IT-PRÜFSTELLE

GUTACHTEN ZUR DSGVO

DATENSCHUTZ IM UNTERNEHMEN

mit Zertifikat . staatlich befugt und beeidigt



Erst-Inspektion mit
Quick-Assessment



Ergebnisse binnen
14 Tagen

Für mehr **Sicherheit, Vertrauen** und **Transparenz**
in der **Informationstechnologie**

ZfP 
IT-PRÜFSTELLE

Inhalt

- Rückblick Webinare DSGVO 2018
- Der IT-Ziviltechniker
- Datenschutzgrundverordnung
- Das Dilemma mit der DSGVO
- Datenschutz-Prüfung
- Datenschutz-Gutachten
- Datenschutz-Zertifikat
- Zusammenfassung



Video >>

IT-Ziviltechniker mit staatlicher Befugnis



HERAUSFORDERUNGEN

- Ordentl. Kaufmann
- Techn. Gesetze
- Techn. Governance
- Techn. Compliance
- Techn. Standards

PROBLEME

- Cybercrime
- IT-Mitarbeiter
- IT-Dienstleister

Admin (!)



DAS PLUS

- Haftung
- ... mit Brief und Siegel
- Zertifikat

IT-Prüf- und Überwachungsstelle
Systeme . Software . Projekte . Datenschutz . IT-Kosten





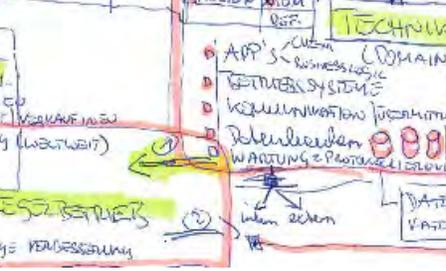
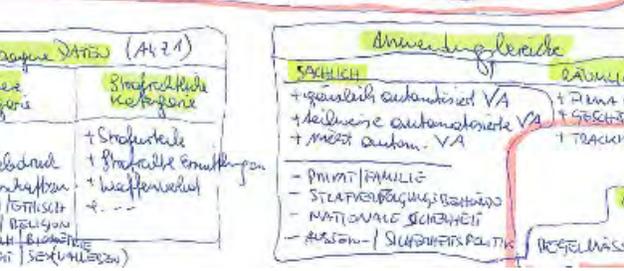
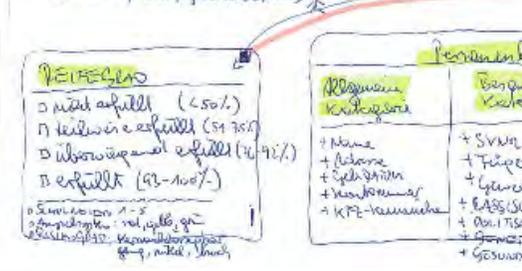
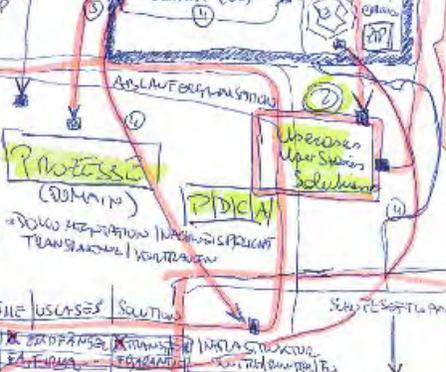
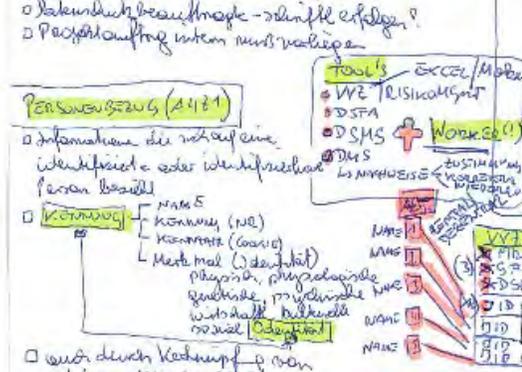
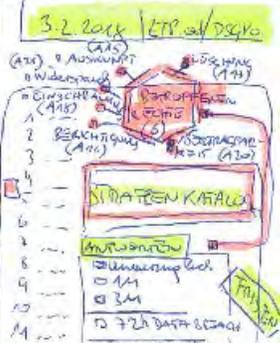
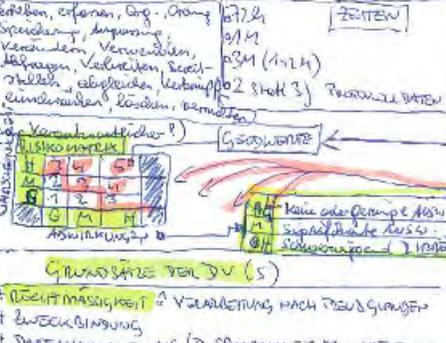
Datenschutz- Grundverordnung DSGVO

DSGVO Strafen

- 204 Mio. Euro gegen British Airways (England)
- 110 Mio. Euro gegen Marriott (England)
- 50 Mio. Euro gegen Google (Frankreich)

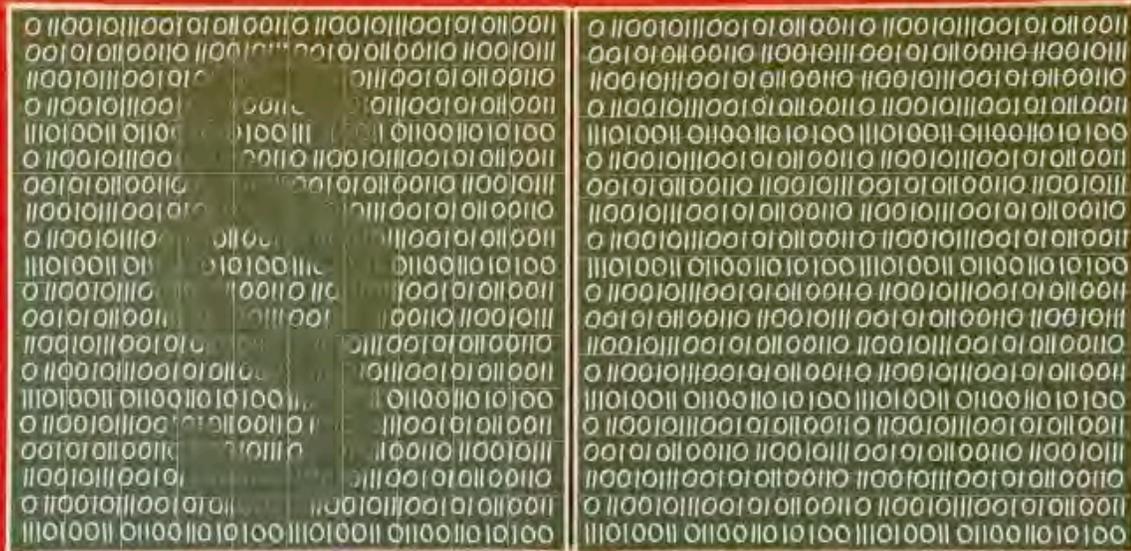
- 18 Mio. Euro gegen die **POST** (AT, Oktober 2019, aufgehoben wegen Formalfehler juristische versus **natürliche Person**)

- Urteil Schrems 2 – Achtung Office 365/Cloud





Das Dilemma mit der DSGVO



Wo versteckte personenbezogene Daten lauern

Böse Überraschung

Martin Gerhard Loschwitz

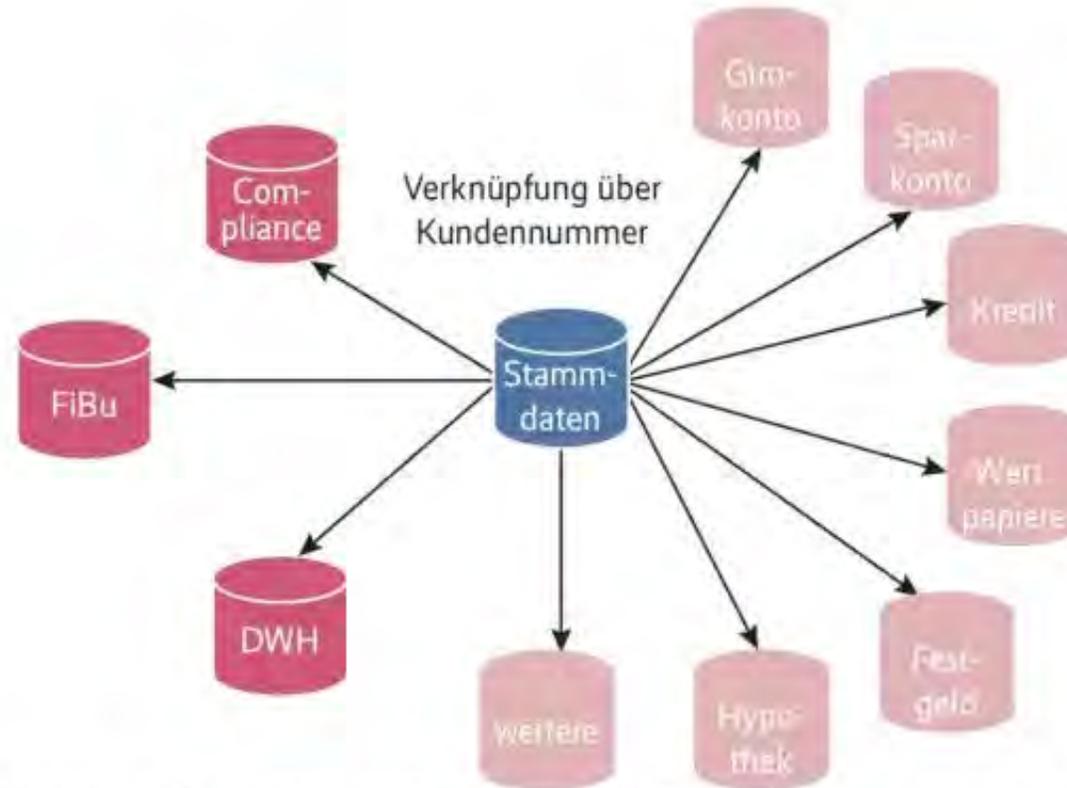
Durch die Löschpflicht der DSGVO können vergessene Datensinken im Unternehmen zu einem echten Problem und verdammt teuer werden. Wo liegen heikle Daten, wie stöbert man sie auf und wie verhält es sich mit WORM-Archiven? iX hilft bei der Spurensuche.



Akribische Untersuchungen sind notwendig

TITEL | LÖSCHEN NACH DSGVO

iX 11/2020 S. 64



So etwa sieht die Systemlandschaft in einer Bank aus. Jedes Datenhaltungssystem speichert nur Teile eines kompletten Datensatzes. Löschen ist hier kompliziert (Abb. 1).

1).

Löschkonzepte gemäß DIN 66398



The screenshot shows the 'INHALTSVERZEICHNIS' (Table of Contents) for DIN 66398. It features a navigation bar at the top with the DIN logo and three menu items: 'Über Normen & Standards', 'Forschung & Innovation', and 'DIN & seine P...'. Below the title, there are expand/collapse controls: '↕ Inhalt' and '↕↕ Alle Ebenen ausklappen' / '↔ Alle Ebenen zuklappen'. The table of contents lists the following sections:

- Vorwort
- Einleitung
- 1 Anwendungsbereich
- 2 Begriffe
- 3 Abkürzungen
- ↕ 4 Grundlagen eines Löschkonzepts
- ↕ 5 Datenarten bilden
- ↕ 6 Löschfristen festlegen
- ↕ 7 Löschklassen
- ↕ 8 Vorgaben für die Umsetzung von Löschregeln
- ↕ 9 Aufbau- und Ablauforganisation: Verantwortung und Prozesse für das Löschen von personenbezogenen Daten
- Anhang A Hinweise für ein Projekt „Löschkonzept“ (informativ)
- Anhang B Hinweise zur Anonymisierung personenbezogener Daten (informativ)
- Anhang C Hinweise zu Vorgaben für die Sicherheit von Löschmechanismen (informativ)
- Anhang D Hinweise zur Sperrung von Datenbeständen (informativ)
- Literaturhinweise (informativ)

Die Leitlinie DIN 66398 enthält Hilfestellungen für die kniffligen Fragen, die sich Unternehmen im Zusammenhang mit DSGVO-konformem Datenlöschen stellen.

Quelle: Deutsches Institut für Normung



ztp.digital



Datenschutzbehörden erklären den Einsatz von Microsoft 365 für rechtswidrig

Was die Datenschutzbehörden Anfang Oktober veröffentlicht haben, bewegt sich irgendwo zwischen unverschämt und weltfremd, findet Heise-Justiziar Joerg Heidrich.

Lesezeit: 4 Min. In Pocket speichern

🔊 🖨️ 💬 24



(Bild: dennizn/Shutterstock.com)

23.10.2020 06:00 Uhr | c't Magazin

Von Joerg Heidrich

ISO 27701 - DSGVO konform?



Erstes Datenschutz-Zertifikat mit internationaler Geltung: ISO 27701 kommt nach Österreich

CIS wurde als erste nationale Prüfstelle akkreditiert – Haftungsminimierung durch Sorgfaltsprinzip.

Wien (OTS) - Während die EU beim Thema Datenschutz hohe Strafen vorsieht, ist eine anerkannte Datenschutz-Zertifizierung bis heute ausständig. Besonders prekär ist dies, weil ein Daten-Eigentümer mithaftet, wenn bei seinem Provider eine Datenpanne passiert und er sich keinen Nachweis für sorgfältiges Vorgehen eingeholt hat. Ohne Zertifizierung war dies bis dato aber schwierig.

JA

ISO 27701 – Endlich eine DSGVO-konforme Datenschutz-Zertifizierung?

27 September, 2019



Die Artikel 42 und 43 der DSGVO regeln, unter welchen Voraussetzungen Zertifizierungen im Datenschutz zulässig sind und welche Anforderungen die Zertifizierungsstellen erfüllen müssen.

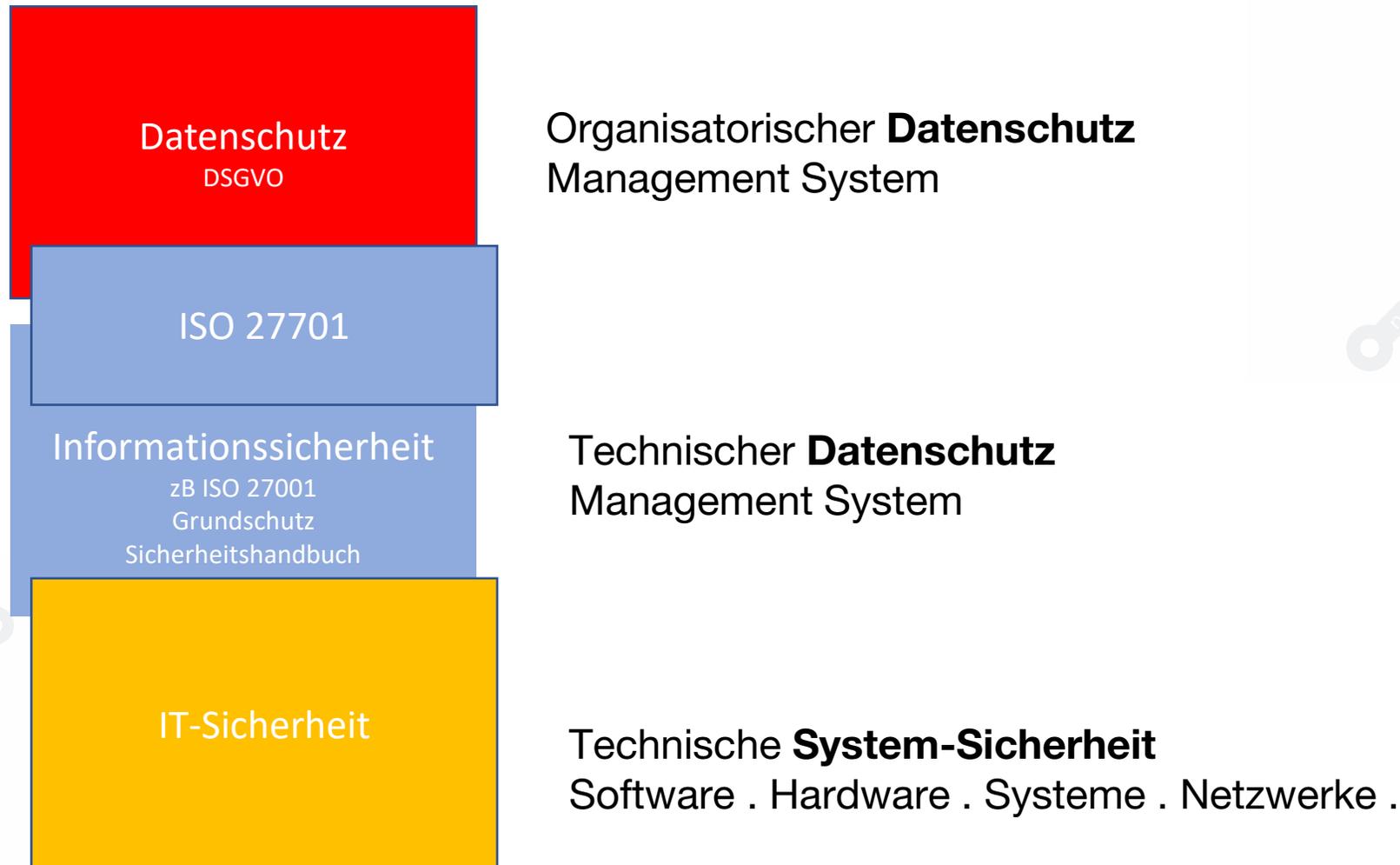
Bei näherer Betrachtung des Artikel 43 ist sofort ersichtlich, dass Datenschutz-Zertifizierungen nur auf Grundlage der ISO 17065 (Zertifizierung von Produkten und Prozessen) möglich sind. Dies bekräftigte das European Data Protection Board in seinen Guidelines zu diesem Thema (Guidelines 1/2018 und Guidelines 4/2018). Zertifizierungen von Datenschutz-Management-Systemen sind somit ausgeschlossen.

Des Weiteren haben ISO-Normen eine entscheidende Schwachstelle, was die Transparenz des Gültigkeitsbereichs beziehungsweise der angelegten Kriterien anbelangt. Oftmals kann anhand des Zertifikates nicht erkannt werden, welche Bereiche tatsächlich zertifiziert wurden. Dies widerspricht den Anforderungen an Datenschutz-Zertifizierungen, die Artikel 42 DSGVO vorgibt.

Fazit: Eine Zertifizierung nach der ISO 27001/27002 in Verbindung mit der ISO 27701 ist nicht DSGVO-konform.

Nein

Datenschutz . Informationssicherheit . IT-Sicherheit



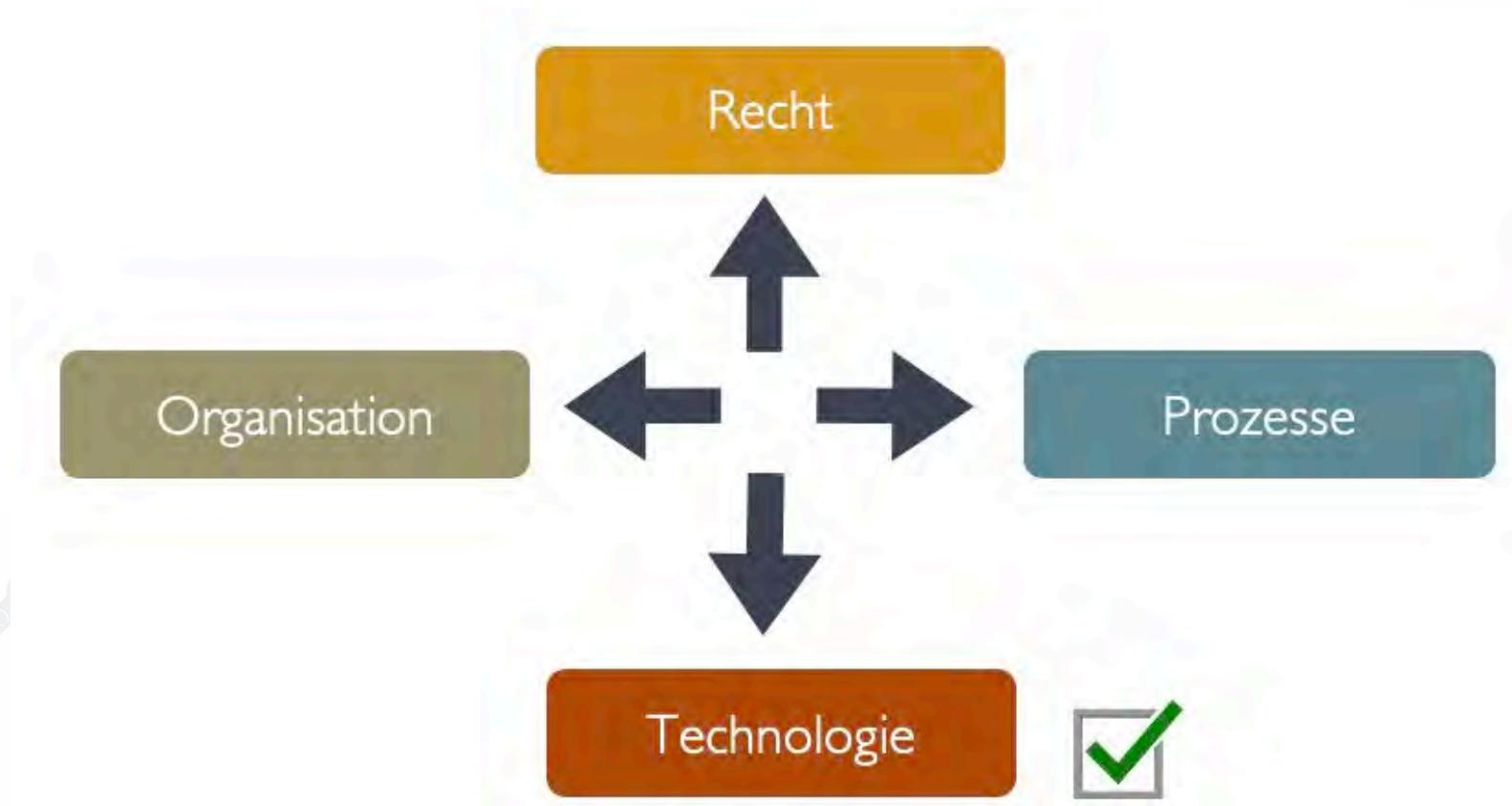


Datenschutz-Prüfung

DSGVO-Architektur



Bereiche der DSGVO



Kontrollpunkte zur DSGVO Zertifizierung

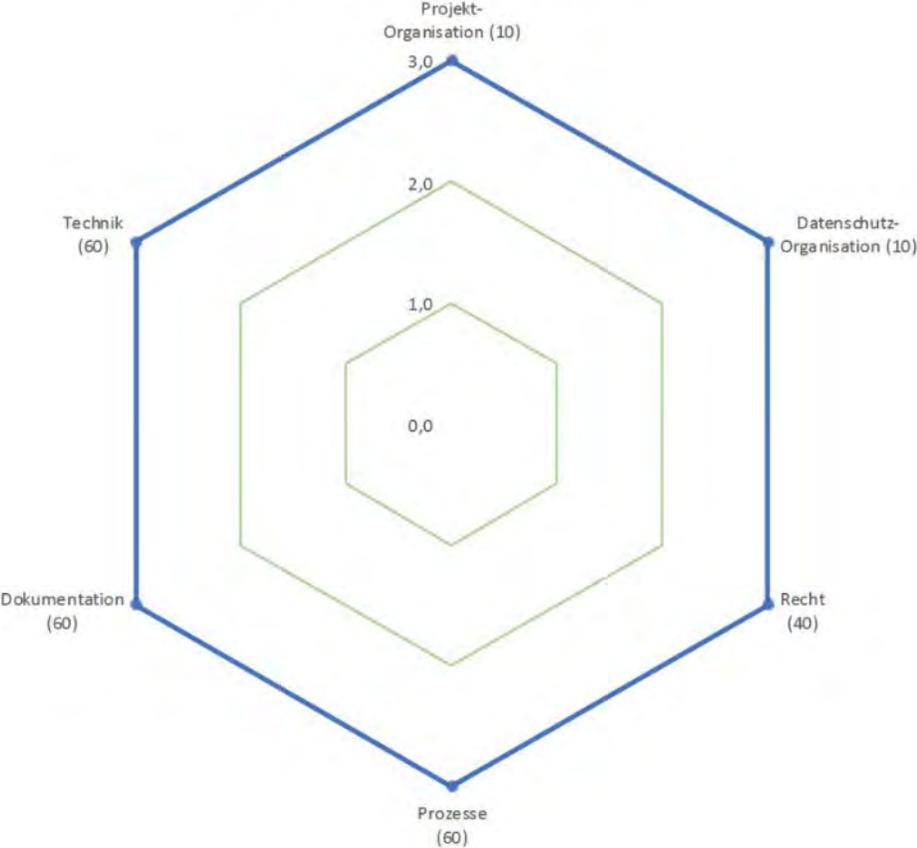
6 Bereiche mit KP - Kontrollpunkten

Projekt-Organisation (10)	KP 1: Projektauftrag vorhanden und unterfertigt?	3	2,8
	KP 2: Projektleiter und Mitarbeiter bestimmt?	3	
	KP 3: Projekt-Organigramm vorhanden?	3	
	KP 4: Projektplan vorhanden?	2	
	KP 5: Projekt-Controlling vorhanden?	3	
Datenschutz-Organisation (10)	KP 6: Datenschutzbeauftragter definiert?	3	2,6
	KP 7: Datenschutz-Organigramm vorhanden?	2	
	KP 8: Kontroll-Gremium vorhanden?	3	
	KP 9: Informationsfluss im Krisenfall definiert?	2	
	KP 10: Geschäftsführung - und Bereichsleitung involviert?	3	
Recht (40)	KP 11: Informationsverpflichtungen (12) auf Homepage, Verträge, Vereinbarungen erfüllt?	3	2,2
	KP 12: Einwilligung(en) notwendig?	2	
	KP 13: Grundsätze (5) der Verarbeitung von personenbezogenen Daten berücksichtigt?	1	
	KP 14: Betroffenenrechte (6) berücksichtigt?	2	
	KP 15: VVT als VA & AV aus rechtlicher Sicht freigegeben?	3	
Prozesse (60)	KP 16: Prozess: Auskunft (2) (Postiv- und Negativfall)?	3	2,7
	KP 17: Prozess: Widerspruch (2) (Postiv- und Negativfall)?	3	
	KP 18: Prozess: Einschränkung (2) (Postiv- und Negativfall)?	2	
	KP 19: Prozess: Berichtigung (2) (Postiv- und Negativfall)?	2	
	KP 20: Prozess: Übertragbarkeit (2)(Postiv- und Negativfall)?	3	
	KP 21: Prozess: Löschung (2) (Postiv- und Negativfall)?	3	
Dokumentation (60)	KP 22: Datenschutzhandbuch vorhanden?	3	2,6
	KP 23: Datenschutzbeauftragter - Rechte und Pflichten dokumentiert?	2	
	KP 24: Verzeichnis der Verarbeitungstätigkeiten vollständig (VVT VA/AV)?	3	
	KP 25: Prozesse ausreichend bewertet und dokumentiert?	2	
	KP 26: IKS durch Wirtschaftsprüfer/STB: bestätigt?	3	
	KP 27: Vorhandene Prüfberichte und Zertifizierungen (ISO 27001, ISO 20000, Cobit, SAE, ...)?	3	
	KP 28: Risikobetrachtung?	2	
	KP 29: Datenschutzfolgeabschätzung (DSVA)?	3	
Technik (60)	KP 30: Inventarisierung der IT-Systeme und Daten(banken) vorhanden?	3	2,6
	KP 31: Netzwerk-Architekturplan vorhanden?	2	
	KP 32: TOM's umgesetzt?	3	
	KP 33: Datenschutz durch Technik umgesetzt?	3	
	KP 34: Datenschutz durch Datenschutz-freundliche Voreinstellung umgesetzt?	2	

Beschreibung	Wert
nicht erfüllt (0-49%)	0
teilweise erfüllt (50-75%)	1
überwiegend erfüllt (76-92%)	2
vollständig erfüllt (93-100%)	3

Assessment

DSGVO-KONTROLLPUNKTE





Datenschutz-Gutachten

Ziviltechnikergutachten

Gutachten und Befund, Version 1.0

GZ: A 100/18, Lfd.Nr.: 54

Datenschutz-Grundverordnung

Inhaltsverzeichnis

1	Allgemeines.....	6
1.1	Ausgangssituation.....	6
1.2	Die Neuerungen.....	6
1.3	Abkürzungen und Begriffsdefinitionen.....	7
1.3.1	Abkürzungen.....	7
1.3.2	Begriffsdefinitionen.....	7
1.4	Gesetzliche und anderweitige Grundlagen.....	14
1.5	Vorgehensmodell.....	14
1.5.1	Beurteilung des angemessenen Schutzniveaus.....	15
1.5.2	Hexagon-Modell.....	15
1.5.3	Reifegradmodell.....	15
1.5.4	Referenzmodell.....	15
2	Auftragnehmer, Auftraggeber und Auftrag.....	16
2.1	Auftragnehmer.....	16
2.2	Auftraggeber.....	16
2.3	Rahmenbedingungen und Restrisiko.....	16
2.4	Prüfauftrag.....	16
2.5	Abgrenzung.....	16
2.6	Unternehmensstruktur.....	17
2.7	Mengengerüste.....	17
3	Beurteilungsgegenstand.....	18
3.1	Zielbilddefinition.....	18
3.1.1	Definition Anwendungsbereich.....	18
4	Ziviltechnikergutachten.....	19
4.1	Projektorganisation.....	19
4.2	Datenschutzorganisation.....	19
4.3	Pflichten des Verantwortlichen.....	19
4.3.1	Verzeichnis von Verarbeitungstätigkeiten.....	19
4.3.2	Technische und organisatorische Maßnahmen.....	20
4.3.3	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.....	21
4.3.4	Meldung von Verletzungen des Schutzes personenbezogener Daten.....	22
4.3.5	Datenschutz-Folgeabschätzung.....	22



4.3.6	Verantwortlichkeiten und Datenschutzbeauftragter.....	23
4.3.7	Pflichten hinsichtlich besonderer Kategorien personenbezogener Daten ..	23
4.3.8	Pflichten als Auftragsverarbeiter	24
4.4	Einhaltung Grundsätze des Datenschutzes.....	25
4.4.1	Rechtmäßigkeit der Verarbeitung.....	25
4.5	Wahrung der Rechte des Betroffenen.....	25
4.5.1	Einhaltung der Transparenz bei der Verarbeitung von personenbezogenen Daten	25
4.5.2	Einhaltung der Rechte auf Information	26
4.5.3	Einhaltung des Rechts auf Auskunft	26
4.5.4	Einhaltung des Rechts auf Berichtigung.....	27
4.5.5	Einhaltung des Rechts auf Löschung	27
4.5.6	Einhaltung des Rechts auf Einschränkung der Verarbeitung	28
4.5.7	Einhaltung des Rechts auf Datenübertragbarkeit	28
4.5.8	Einhaltung des Rechts auf Widerspruch.....	29
4.6	Zusammenfassung	29
4.7	Weitere Schritte - Datenschutzzertifizierung	30
5	Befund.....	31
5.1	Projektorganisation	31
5.2	Datenschutzorganisation	32
5.2.1	Datenschutzhandbuch.....	32
5.3	Datenschutzrechtliche Abgrenzung (Art. uA 2, 3, 23, 26, 40; DSGVO § 36ff)	34
5.4	Pflichten des Verantwortlichen.....	34
5.4.1	Verzeichnis von Verarbeitungstätigkeiten (Art. 30)	34
5.4.2	Technische und organisatorische Maßnahmen (vgl. Art 24, 32; DSGVO § 13) ..	36
5.4.3	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25)	38
5.4.4	Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33, 34) ..	39
5.4.5	Datenschutz-Folgeabschätzung (Art. 35, 36)	43
5.4.6	Verantwortlichkeiten und Datenschutzbeauftragter (Art. 37, 38, 39; DSGVO § 5).....	44
5.4.7	Pflichten hinsichtlich besonderer Kategorien personenbezogener Daten (Art. 9) ..	47
5.4.8	Auftragsdatenverarbeitungen (Art 28)	48
5.5	Einhaltung Grundsätze des Datenschutzes.....	49

5.5.1	Rechtmäßigkeit der Verarbeitung (Art. 6; DSGVO § 7-11; § 12)	49
5.6	Wahrung Rechte des Betroffenen.....	50
5.6.1	Einhaltung der Transparenz bei der Verarbeitung von personenbezogenen Daten (Art. 12)	50
5.6.2	Einhaltung der Rechte auf Information (Art. 13,14)	52
5.6.3	Einhaltung des Rechts auf Auskunft (Art 15).....	54
5.6.4	Einhaltung des Rechts auf Berichtigung (Art. 16, 19).....	56
5.6.5	Einhaltung des Rechts auf Löschung (Art. 17, 19; § 4 DSGVO).....	57
5.6.6	Einhaltung des Rechts zur Einschränkung der Verarbeitung (Art. 18)	59
5.6.7	Einhaltung des Rechts auf Datenübertragbarkeit (Art. 20).....	60
5.6.8	Einhaltung des Rechts auf Widerspruch (Art. 21).....	62
5.6.9	Einhaltung der Verpflichtung durch den bzw. als Auftragsverarbeiter (Art. 28) ..	62
6	Anhang	65
6.1	Dokumentenverzeichnis	
6.2	Sonstiges.....	
6.2.1	Übersetzung Datenschutzrelevanter Begriff aus der Verordnung (Deutsch/Englisch)	
6.3	Referenz Kontrollpunkte	
6.4	Fragebögen	
6.5	Technische Berichte.....	
6.5.1	Prüfung Website	
6.5.2	Prüfung Cookies.....	
6.5.3	Prüfung zentrale Intranet Systeme /	
	technisch organisatorischer Bericht.....	
6.6	Protokolle und Sonstiges	
6.6.1	Protokolle.....	
6.6.2	Projektfortschrittsüberwachung – Gantt Chart.....	
6.6.3	Zertifizierungen	
6.6.4	Betroffenenrechte	
6.6.5	GAP-Analyse	





Datenschutz-Zertifikat

zt:

MUSTER-ZERTIFIKAT

EU-Datenschutz-Grundverordnung

für

MUSTER GMBH

Musterfirma Gesellschaft m.b.H.
0000 Musterstadt, Musterstraße 00, www.musterfirma.at

Prüfung der geeigneten technischen und organisatorischen
Maßnahmen gem. Art. 25 und Art. 32 der EU-Datenschutz-Grundverordnung (DSGVO)

Überwachungszeitraum

1. Februar 2021 bis 31. Jänner 2022

Bestätigt gemäß Ziviltechnikergesetz¹



ZTP.digital . Prüfstelle für Digitale Sicherheit
CEO ZT DI Dr.techn. Wolfgang Prentner, staatlich befugt und besidet
ZTP.digital ZTP-GmbH, Wistranergasse 40/3/3 Wien, NÖ, VB
T: +43 1 532 46 86 0 | www.ztp.digital | office@ztp.digital | ztp.digital

ZT DI Dr.techn. Wolfgang Prentner
staatlich befugt geprüft

Wien, 01. Februar 2021



¹ Ziviltechnikergesetz 1993, §4 Abs.3.: Ziviltechniker sind mit öffentlichem Glauben versehene Personen gemäß §292 Zivilprozeßordnung, RGBI. Nr. 113/1895, in der jeweils geltenden Fassung. Die von ihnen im Rahmen ihrer Befugnis ausgestellten öffentlichen Urkunden werden von den Verwaltungsbehörden in derselben Weise angesehen, als wenn diese Urkunden von Behörden ausgefertigt wären. Unter Berücksichtigung von ÖNORM 7700, BSI Websicherheit, ISO 27001.



Zusammenfassung

GUTACHTEN

ZUR **DSGVO**

DATENSCHUTZ

IM **UNTERNEHMEN**

mit Zertifikat . staatlich befugt und beeidigt



Unabhängig.

Planen. Prüfen.

Nur sicher mit dem Siegel.
Ihre ZiviltechnikerInnen.



Erst-Inspektion mit
Quick-Assessment



Ergebnisse binnen
14 Tagen

Für mehr **Sicherheit, Vertrauen** und
in der **Informationstechnologie**

ZITP 
IT-PRÜFSTELLE



Besten Dank
für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?





Gesundheit für Ihre IT. ■

ZTP.digital ZT-GmbH

T: +43 1 532 46 68 0

✉ office@ztp.digital

Wien . Niederösterreich . Vorarlberg

Prüfstelle für
Digitale Sicherheit

F: +43 1 532 46 68 - 20

🌐 www.ztp.digital

Austria . Europe

Nicht erlaubte Tätigkeiten



Keine
kommerzielle
Entwicklung von
Software



Keine
kommerzieller
Verkauf von
Hardware oder
Software



Keine
kommerzieller
Betrieb eines
Rechenzentrums

Kunden von ztp.digital



Kunden von ztp.digital

